UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,887	06/20/2003	Gerard Marmigere	FR920020034US1	6788

23550 7590 05/15/2007
HOFFMAN WARNICK & D'ALESSANDRO, LLC
75 STATE STREET
14TH FLOOR
ALBANY, NY 12207

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/600,887	MARMIGERE ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso T-G	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,6,8-12,15 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,6,8-12,15 and 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a final-Office Action in response to the applicant's communication filed on February 23, 2007.

2. The applicant added new claims 15 and 16.

3. Claims 1,3,6,8-12,15, and 16 have been considered and are pending.

Response to Arguments

4. Applicant's arguments filed February 23, 2007 have been fully considered but they are not persuasive.

The applicant argues, "Jobs fails to disclose that **only the IMEI number is used as a shared key** for the encryption of the text data field content. Rather, Jobst discloses that the combination of the IMEI number and the Master Password is encrypted using an undisclosed public/ shared key." The examiner disagrees with the applicant's argument because as admitted by the applicant in the argument Jobs teaches the user of both IMEI and Master password to generate a secure phone password and later used in calculating downloaded code digital signature (see Jobst figure 4: 37, 38, 40 and 43). By simply reducing or eliminating the features disclosed by Jobst which is removing "Master Password and this case and applying "only the IMEI" is an features reeducation or modification of Jobst teaching.

For the above given reasons, the applicant's argument is not persuasive do not overcome the prior arts in record to place the claims in condition for allowance. Therefore independent claims 1 and 11 are not placed in condition for allowance over prior arts in record. Dependant

claims 3, 6, 9 and 12, depending directly or indirectly from their corresponding independent claims are also not placed in condition for allowance.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3, 6, 9, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jobst et al. (US Pat. No.: 6,707,915) in view of Koukoulidis et al. (US Pub. No.: 2003/0123669), and further in view of Stephenson et al. (US Pat. No.: 6, 119, 000).

As per claim 1:

Jobst et al. disclose a text messaging system for the encryption of at least one text. message sent to a wireless terminal equipment, the text message comprising a Short Message Service (SMS) message having a User Data Header (UDH) an information data field and a text data field, the text messaging system comprising:

means for storing an equipment identification number uniquely assigned to the wireless terminal equipment, wherein the assigned equipment identification number is an International Mobile Equipment Identity (IMEI) number of the wireless terminal equipment (Column 6: lines 31-47; Column 7: lines 5-15; Figure 3; figure 5: 1);

means coupled to the equipment identification number storing means for encrypting the text data field content of the SMS message using only the equipment identification number assigned to the wireless terminal equipment as the shared key (Column 2: lines 20-45; Column 6: lines 57-67; Column 7: lines 1-36);

and means for setting an encryption identifier in the information data field of the at least one text message (Figure 8: 63,64,65,66).

Jobst et al. do not explicitly teach the encryption and decryption system is carried out using Short Message Service (SMS) system. Koukoulidis et al., in an analogous art teach the encryption and decryption process is carried out using Short Message Service (SMS) system (Figure 2A: 20; Figure 4: 460; Figure 5: 20; Page 1: 0018). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Jobst et al. to include encryption and decryption process is carried out using Short Message Service (SMS) system. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to secure transaction and communication utilizing SMS as suggested by suggestion provided by Koukoulidis et al. (Page 1: 0005, 0007,0018).

Jobst and Koukoulidis do not explicitly teach an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a

length of the marker. Stephenson et al., in an analogous art, teach an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker (column 11: lines 35-55;column 12: lines 60-67; column 13: lines 1-5; column 19: lines 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Jobst and Koukoulidis to include an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a method of tracking identity-code in a communication system in which a plurality of user stations can simultaneously conduct respective communication transaction during which signaling messages are exchanged with the remainder of the communication system as suggested in (column 2: lines 1-10).

As per claim 3:

Jobst et al. disclose a system, wherein the text data field of the SMS message comprises configuration commands to remotely manage the wireless terminal equipment (Column 6: lines 20-30; Column 2: lines 1-13).

As per claim 6:

Koukoulidis et al. disclose a system, wherein wireless terminal equipment is a Short Message Service (SMS) receiving mobile device and said SMS message is carried over a wireless network (Figure 4: 400; 460).

As per claim 9:

Koukoulidis et al. disclose a system, wherein the means for generating an encrypted SMS message further comprising means for processing an encryption algorithm to compute a bit string using said assigned equipment identification number as the shared key and the text data field content (Page 2: 0032).

As per claim 11:

Jobst et al. disclose a method for authenticating a text message sent by a text messaging system to a wireless terminal equipment (Column 10: lines 33-49; Figure 7) having means for storing International Mobile Equipment Identity (IMEI) number (Column 6: lines 31-47; Column 7: lines 5-15; Figure 3; figure 5: 1) the text messaging system (Column 5: lines 10-21) comprising:

means for storing International Mobile Equipment Identity (IMEI) number, the text message system comprising means for storing an IMEI number uniquely assigned to the wireless terminal equipment (Column 2: lines 20-45; Column 6: lines 57-67; Column 7: lines 1-36), and

wherein the text message comprises a Short Message Service (SMS) message having a User Data Header (UDH) and a text data field, the method comprising the steps of:

at the text messaging system (Column 5: lines 10-21):

encrypting the text data field content by using the equipment identification number assigned to the wireless terminal equipment as the shared key (Figure 8: 65);

setting an encryption identifier An Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker (Figure 7: 206); and

sending the encrypted SMS message to the wireless terminal equipment (Figure 5: 41);

at the wireless terminal equipment (Figure 5: 1; Phone);

receiving the encrypted SMS message (Figure 7: 205);

determining if the received encrypted at least one text message contains an IMEI number as a shared key encryption (Figure 7: 208); and

decrypting the received encrypted SMS message using the IMEI number of said wireless terminal equipment as a shared key (Column 11: lines 50-59).

Jobst et al. do not explicitly teach the encryption and decryption process is carried out using Short Message Service (SMS) system. Koukoulidis et al., in an analogous art teach the encryption and decryption process is carried out using Short Message Service (SMS) system (Figure 2A: 20; Figure 4: 460; Figure 5: 20; Page 1: 0018). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Jobst et al. to include encryption and decryption process is carried out using Short Message Service (SMS) system. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to secure transaction and communication utilizing SMS as suggested by suggestion provided by Koukoulidis et al. (Page 1: 0007).

Jobst and Koukoulidis do not explicitly teach an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker. Stephenson et al., in an analogous art, teach an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker (column 11: lines 35-55;column 12: lines 60-67; column 13: lines 1-5; column 19: lines 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Jobst and Koukoulidis to include an Information Element (IE) group of the UDH of the SMS message, the encryption identifier comprising a marker in an IE data field, the IE group further comprising an information Element Identifier (IEI) field set to indicate a presence of the marker, and an Information Element Data Length (IEDL) field set to indicate a length of the marker. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a method of tracking identity-code in a communication system in which a plurality of user stations can simultaneously conduct respective communication transaction during which signaling messages are exchanged with the remainder of the communication system as suggested in (column 2: lines 1-10).

As per claim 12:

Jobst et al. disclose a method of determining if the encrypted SMS message contains configuration commands to remotely activate the wireless terminal equipment (Column 4: lines 40-51).

7. Claims 8, 10, 15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jobst et al. (US Pat. No.: 6,707,915) in view of Berry et al. (US Pub No.: 2001/0039620)

As per claim 15:

Jobst et al. a text messaging system for the encryption of a text message sent to a wireless terminal equipment, the text message comprising a Short Message Service (SMS) message, the text messaging system comprising:

means for storing an equipment identification number uniquely assigned to the wireless terminal equipment, wherein the assigned equipment identification number is an International Mobile Equipment Identity (IMEI) number of the wireless terminal equipment (Column 6: lines 31-47; Column 7: lines 5-15; Figure 3; figure 5: 1);

means coupled to the equipment identification number storing means for encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key (Column 2: lines 20-45; Column 6: lines 57-67; Column 7: lines 1-36);

means for setting an encryption identifier(Figure 8: 63,64,65,66);

means for storing an IMEI number (column 6: lines 56-67);

means for receiving the encrypted SMS message (Figure 7: 205);

means for determining if the received encrypted SMS message contains an IMEI number as a shared key encryption (Figure 7: 208);

means for decrypting the received encrypted SMS message using the stored IMEI number of said wireless terminal equipment (Column 11: lines 50-59).

Jobst et al. do not explicitly teach means for decrypting the received encrypted SMS message using the stored IMEI number of said wireless terminal equipment. Berry et al., in an analogous art teach means for decrypting the received encrypted SMS message using the stored

IMEI number of said wireless terminal equipment (0020; 0021). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Jobst et al. to include means for decrypting the received encrypted SMS message using the stored IMEI number of said wireless terminal equipment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a memory device in which no-one can process the information contained in the memory card without the password or the electronic device with the correct IMEI code as suggested by Berry in (0001, 007).

As per claim 8:

Jobst et al. disclose a system, comprising means coupled to the decrypting means for processing or rejecting the decrypted at least one text message (Figure 7: 208, 209).

As per claim 10:

Berry et al. disclose a system, wherein the means for decrypting the received encrypted at least one text message further comprising means for processing a decryption algorithm using said personal equipment identification number as the shared key and the received encrypted at least one text message content (0020; 0021).

As per claim 16:

Jobst et al. a method for authenticating a text message sent by a text messaging system to a wireless terminal equipment having means for storing an International Mobile Equipment

Identity (IMEI) number, the text messaging system comprising means for storing an IMEI number uniquely assigned to the wireless terminal equipment, and wherein the text message comprises a Short Message Service (SMS) message, the method comprising:

at the text messaging system (Column 5: lines 10-21):

encrypting the text data field content of the SMS message using only the IMEI number assigned to the wireless terminal equipment as the shared key(Figure 8: 65);

setting an encryption identifier in the SMS message (Figure 7: 206); and

sending the encrypted SMS message to the wireless terminal equipment;

at the wireless terminal equipment (Figure 5: 1; Phone):

receiving the encrypted SMS message (Figure 7: 205).

Jobst et al. do not explicitly teach means for decrypting the received encrypted SMS message using the stored IMEI number of said wireless terminal equipment and processing or rejecting the decrypted SMS message based on the decryption result. Berry et al., in an analogous art teach means for decrypting the received encrypted SMS message using the stored IMEI number of said wireless terminal equipment processing or rejecting the decrypted SMS message based on the decryption result. (0020; 0021). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Jobst et al. to include means for decrypting the received encrypted SMS message using the stored IMEI number of said wireless terminal equipment processing or rejecting the decrypted SMS message based on the decryption result. This modification would

have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a memory device in which no-one can process the information contained in the memory card without the password or the electronic device with the correct IMEI code as suggested by Berry in (0001, 007).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T-G

Techane Gergiso

Patent Examiner

Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

May 11, 2007